Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	January 1, 2022

Data Classification

Information and Technology

Contents

I. Introduction

A. **Authority:** Colorado Revised Statutes (C.R.S.) § 23-54-102, *et seq.* (2022) authorizes the Trustees of Metropolitan State University of Denver ("MSU Denver" or "University") to establish rules and regulations to govern and to operate the University and its programs. The MSU Denver Trustees retain authority to approve, to administer, and to interpret policies pertaining to University governance. The MSU Denver Trustees authorize the MSU Denver President to approve, to administer, and to interpret policies pertaining to University operations.

B. **Purpose:** MSU Denver's information security policies are focused on protecting critical data and information systems of Metropolitan State University of Denver from loss, damage, or inappropriate modification or disclosure. The purpose of this policy is to educate the University community about the importance of protecting data generated, accessed, transmitted, received, and stored by the University, to identify procedures that should be in place to protect the confidentiality, integrity, and availability of University data, and to comply with local and federal regulations regarding privacy and confidentiality of information.

C. **Scope:** This policy applies to all individuals, including students, faculty, staff, and contractors provided access to University data and information technology systems. Contractors and otherwise affiliated individuals must agree to abide by the information security policies before accessing University systems and data. Role-based policies and procedures that apply to specific groups of users will be provided when applicable, in accordance with functional requirements and data classification.

Data Classification

Information and Technology

II. Roles and Responsibilities

A. **Responsible Executive:** Chief Information Officer

B. **Responsible Administrator:** Chief Information Security Officer

C. **Responsible Office:** Information Technology Services

D. **Policy Contact:** IT Services, www.msudenver.edu/technology , 303-352-7548

E. **Additional Roles and Responsibilities:**

1. The Chief Information Security Officer is charged with the promotion of security awareness within the University community, as well as responsibility for the creation, maintenance, enforcement, and design of training on relevant security standards in support of this policy. The Chief Information Officer will receive and maintain reports of incidents, threats, and malfunctions that may have a security impact on the University's information systems and will receive and maintain records of actions taken or policies and procedures developed in response to such reports. The Chief Information Officer will assist with internal audits, as appropriate, to determine compliance with this policy.
2. MSU Denver IT Services will facilitate distribution of this policy, will assist in the investigation of policy breaches, and will respond promptly to reports of suspected misconduct or violations of law or University policies.
3. The Office of General Counsel will review procedures issued under authority of this policy for compliance with applicable regulations. The Office of General Counsel will also respond to court-ordered releases of information.

Data Classification

Information and Technology

III. Policy Statement

A. **Responsibility for Data Management.** Data is a critical asset of the University. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, received, stored, or used by the University, irrespective of the medium on which the data resides and regardless of format, such as in electronic, paper, or other physical form. Individual departments are responsible for following appropriate managerial, operational, physical, and technical controls for access to, use of, verbal or electronic transmission of, and disposal of University data in compliance with this policy. Data owned, used, created, or maintained by the University and University personnel is classified into the following three categories:

1) Public,

2) Official Use Only,

3) Confidential.

Departments and administrative branches should carefully evaluate the appropriate data classification category for information handling within their environment. When provided in this policy, examples are illustrative only and serve as identification of implementation practices rather than specific requirements. Nothing in this policy is intended to identify a restriction on the right of departments or administrative branches to require policies and/or procedures in addition to the ones identified in this document. This policy does not apply to individuals' handling of their own confidential information.

B. **Data Classification**

1. **Public Data.** Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. By way of illustration only, some

examples include: Publicly posted press releases; Publicly posted schedules of classes; Publicly posted interactive University maps, newsletters, newspapers, and magazines.

2. **Official Use Only Data.** Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.
    a. By way of illustration only, some examples of Official Use Data include:
        i. Employment data;
        ii. University partner or sponsor information when no more restrictive confidentiality agreement exists; and
        iii. Internal telephone books and directories.
    b. Official Use Only Data:
        i. Must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
        ii. Physical copies must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
        iii. Electronic files must not be stored in unsecure locations, on PCs or other hardware, nor posted on any publicly accessible website.
        iv. Must be destroyed when no longer needed subject to University and/or departmental Records Retention Schedules. Destruction may be accomplished by:
            a) "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.

b) Electronic storage media shall be sanitized appropriately by overwriting or physical destruction prior to disposal. Disposal of electronic equipment must be performed in accordance with IT Service's surplus equipment process.

3. **Confidential Data.** Confidential Data is information protected by statutes, regulations, University policies, or contractual language. Managers may also designate data as confidential. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the University should be authorized by executive management.
    a. By way of illustration only, some examples of Confidential Data include:
        i. Medical records
        ii. Student records and other non-public student data
        iii. Social Security Numbers
        iv. Non-public Personnel and/or payroll or records
        v. Bank account numbers and other personal financial information
        vi. Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
    b. Confidential data:
        i. When stored in an electronic format, must be protected with strong passwords and stored on systems that utilize protection and encryption measures approved by MSU Denver IT Services in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.
        ii. Must not be transmitted through standard email. All transfer or sharing of confidential data must be performed using MSU Denver IT Services managed secure file transfer and sharing systems.
        iii. Must not be disclosed to parties without explicit management authorization or appropriate contracts.

iv. Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

v. When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.

vi. Must not be posted on any public website.

vii. Must be destroyed when no longer needed subject to the University Records Retention Schedule. Destruction may be accomplished by:

a) "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.

b) Electronic storage media shall be sanitized appropriately by overwriting or physical destruction prior to disposal. Disposal of electronic equipment must be performed in accordance with IT Service's Surplus Equipment Process.

c. References to intellectual property exclude faculty and do not preclude standing policies.

d. The Chief Information Security Officer must be notified in a timely manner if data classified as confidential is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place. The Chief Information Security Officer must notify the University President of said loss or disclosure, with notifications to other parties as required.

C. **Procedures:** Individuals should contact the IT Service Desk to report security risks, violations of policy, or to make requests for exceptions or amendments to the policies. The Chief Information Security Officer (CISO) and other IT Services staff will respond to all reported security issues and will work with the policy subcommittee to allow for development of appropriate updates to policies.

D. **Sanctions:** Adherence to MSU Denver information-security policies is mandatory and may be based on state or federal statute, contract language, or information-security standards. These policies are not intended to unreasonably interfere with system utilization. Violations of these policies may result in fitting administrative action up to and including revocation of system privileges, employee termination, or student expulsion.

IV. Related Information

A. Family Educational Rights and Privacy Act of 1974 (FERPA) http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
B. Health Insurance Information Portability and Accountability Act (HIPAA) http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
C. PCI Security Standards https://www.pcisecuritystandards.org/security_standards/index.php https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
D. MSU Denver Website Privacy Statement, https://www.msudenver.edu/privacy/

V. History

A. **Effective:** January 1, 2022
B. **Enacted:** July 1, 2017
C. **Review Schedule:** This policy will be reviewed every three years or as deemed necessary by University leadership.

Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	January 1, 2022

Data Classification

Information and Technology

VI. Approval

Janine Davidson, Ph.D.
President, Metropolitan State University of Denver

N/A

Chair, Board of Trustees, Metropolitan State University of Denver